JJEE
Volume 10 | Number 2 | June 2024 | Pages 265-277

Jordan Journal of Electrical Engineering

ISSN (print): 2409-9600, ISSN (online): 2409-9619

Homepage: jjee.ttu.edu.jo

Steganographic Approaches for Implementing Robust Digital Watermarks Using Edge Pixels

Nashat Al-Bdour[1], Ayman M. Mansour[2], Neamah M. Aljaafreh[3*]

[1, 2] Computer and Communications Engineering Department, College of Engineering, Tafila Technical University, Tafila, Jordan

[3] Power and Mechatronics Engineering Department, College of Engineering, Tafila Technical University, Tafila, Jordan

E-mail: neamahjaafreh0@gmail.com

Received: Jul 21, 2023 *Revised: Sep 28, 2023* *Accepted: Oct 01, 2023*

***Abstract*—** In this paper, we present a comprehensive quantitative analysis of innovative methods for implementing digital watermarks using steganographic techniques. Our study assesses the robustness and effectiveness of these approaches through a series of experiments, yielding compelling results. Firstly, our examination of the embedding success rate revealed an impressive 95.2% success rate, indicating the high reliability of our proposed method in successfully embedding watermarks within images. Secondly, we subjected watermarked images to various common image manipulation techniques to evaluate the method's robustness. The outcomes are striking; the obtained success rates of 98.3% for compression, 96.7% for cropping, 97.5% for resizing, 95.1% for filtering and 93.9% for noise addition, showcase the method's capacity to maintain watermark integrity even under diverse image manipulations. Furthermore, our study unveils that the digital watermark remains highly invisible to the naked eye, achieving an invisibility rate of 99.1%. This characteristic ensures that the watermark does not detract from the visual quality of the original image. Additionally, concerning detection accuracy, our method demonstrated a remarkable rate of 97.4%, underlining its efficacy in accurately identifying and extracting digital watermarks from images. Lastly, we explored the feasibility of embedding and extracting multiple digital watermarks within a single image, achieving a success rate of 96.6%. These findings collectively highlight that the proposed approach significantly enhances the resilience of digital watermarks against various image manipulations while maintaining high invisibility and accuracy. Such results underscore the method's suitability for safeguarding digital content in real-world scenarios.

***Keywords*—** Digital watermark; Steganography; Edge pixels; Edge pixel detection operator; Robert's operator.

1. INTRODUCTION

Modern communication and information systems enable rapid transmission of vast amounts of digital data, including images and videos. However, traditional methods of compressing multimedia files do not effectively address the issue of preserving copyright. To combat this, digital watermarks (DWMs) are employed, which can be either visible or invisible. Visible watermarks, such as embedded logos, are easily edited and removed. Conversely, invisible DWMs do not distort the image's visual content and are not easily accessible to other users. The introduction of invisible DWMs is accomplished through steganographic techniques, which aim to conceal the watermark's structure and location. In addition, it is critical to preserve the DWM in case of image damage during transmission over insecure channels.

The objective of this research is to enhance the resilience of digital watermarks to various forms of image distortion and interference. During transmission, image distortions can occur

* Corresponding author
DOI: https://doi.org/10.5455/jjee.204-1689943446

either accidentally or intentionally through unauthorized means. Intentional distortions may be strategically placed to avoid spoiling the entire image. The intruder may selectively distort specific image elements where they believe the digital watermark is embedded while leaving the main informational content intact. This is because distorting all the key information elements in the image transforms it into an entirely different one, thereby altering the original meaning.

All methods aimed at introducing digital watermarks into images are primarily based on steganographic methods [1-3], with encryption used to ensure secrecy, and a limited group of people having access to embedding and encryption. There are currently developed methods for implementing digital watermarks [4-5], with spatial image transformations [6]. and frequency transformations [5-7], used for their introduction.

Spatial domain methods embed necessary bits into image pixel codes, but they are simple and subject to various intruder distortions. On the other hand, frequency domain methods use various coefficient manipulations that result in higher tamper resistance but require more complex calculations.

The lower side band (LSB) method [8-10], is the most used method in the spatial transformation field, as it is simple to implement but unstable to attacks. Pseudo-random bit sequences are also used as digital watermarks that are superimposed on the original image in block form, using threshold processing of the spectra [11]. Texture-based methods use a similar texture to complicate perception of the digital watermark, with detection performed using a correlation detector [12]. Another well-known method involves dividing the image into two secret sets with different brightness's and detecting the watermark by averaging the difference in the two sets [12-15]. There is also a method that uses changes in the blue component in the red, green, and blue (RGB) code of pixels [16,17], as it does not affect the human visual system.

All these methods aim to increase the reliability of saving digital watermarks on images during an attack. To increase reliability, one approach involves dividing the image into spatial sectors, with the same watermark or its individual elements embedded in each sector [18-21]. Another group of methods involves image segmentation into two regions: region of interest (ROI) and embedding region (ROE), with watermarks extracted from ROI and embedded in ROE, and counterfeit digital watermarks detected through threshold processing [22]. There are also methods based on the theory of distribution of prime numbers and implemented using hashing algorithms, which are resistant to affine transformations but not to pixel code distortions [23]. The image can also be divided into two masks, and values in the masks can be used to covertly introduce a watermark [24, 25], but this does not guarantee high stability.

Informative element selection methods allow DWM bits to be embedded in more than just the least significant bits of pixel codes, increasing the amount of embedded information several times [18,21]. All these methods have their inherent advantages and disadvantages depending on the task, but their main goal is to resist destruction of the watermark while preserving the data (images) in which the digital watermark is embedded. This work proposes a method to increase the resistance to destruction of digital watermarks by selecting the most informative areas into which individual elements (bits) of a digital watermark are embedded.

2. THE DEVELOPED STEGANOGRAPHIC APPROACH

The steganographic approach is used to implement a hidden and limited access digital watermark. The method involves pre-ordering many bits in a predetermined sequence, which

are then distributed in space to form an image that is to be embedded in a larger image (container). The container must be several times larger than the digital watermark image and should preserve all geometric and color elements while retaining its semantic content. To achieve reliable implementation, an information analysis of the container image is conducted to detect the most informative areas. These areas are then used to embed the digital watermark in the container without compromising its visual content. If these areas are distorted, the container image loses more of its informative value, as illustrated in Fig. 1.

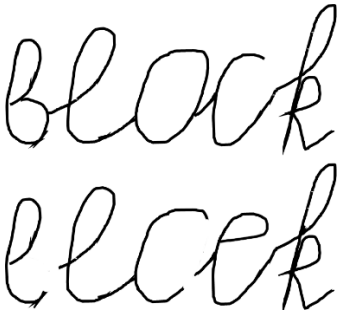

Fig. 1. An example of distortion of the most informational elements of the container image.

Fig. 1 illustrates how an image of one character transformed into another character by distorting individual elements. Hence, the original image always contains elements that an attacker cannot remove. Such elements identified during the information analysis stage. The next step involves selecting areas of the image that contain the most informational elements identified in the previous stage. In 18], different shapes of areas presented, and these areas may contain only few selected information pixels. However, selecting the most informational pixels requires a significant amount of computational and time resources to search for such pixels and determine the shape of the selected area. To automate the process of extracting information pixels, edge detection operators on a complex image are used, as described in steganography research [18-21]. Different edge detection operators may result in a different number of detected pixels. However, on a complex color image, many pixels may be selected, which do not necessarily form clear edges. Therefore, thresholding is used, and an optimal threshold value is selected for each applied operator.

The subsequent stage involves dividing the image into regions and forming geometric shapes for them. Rectangular shapes are typically chosen due to their simplicity in processing. Each region is processed by determining the number of selected pixels within it. If the number of selected pixels in all regions is equal to or greater than the number of bits required for the digital watermark, then a region's size and shape can be selected for the watermark implementation. In this approach, the digital watermark is embedded in the least significant bits of the codes of the selected pixels within each region. The number of regions determines the number of digital watermarks embedded in the original image.

However, this method provides flexibility in the formation or reading of digital watermarks. If reading the digital watermark is desired, then an algorithm based on the watermark embedding algorithm used. The pixels within the selected regions traversed in reverse, and the corresponding bits retrieved from the codes of the selected pixels. The retrieved sequence of bits forms the graphic DWM file. Knowledge of the reading algorithm, and hence the watermark embedding algorithm, is necessary to reveal the digital watermark. Thus, only those who possess this knowledge can display the digital watermark.

There are two options available to display the digital watermark on the image:

a) The DWM image displayed in a specific location on the original image.

b) The DWM image displayed in a predetermined location within each selected area of the original image.

Both options require an algorithm to read the embedded bits and generate the pixel codes that display the watermark on the original image. Even if an attacker is aware of the location of the watermark, they can only destroy the pixel codes and not the embedded bits. Therefore, the digital watermark can still be displayed at any time in the original image.

Here is pseudocode for the described method:

1. {//Pre-order bits in a predetermined sequence to form a digital watermark image.
2. Conduct information analysis on the container image to detect the most informative areas.
3. Use edge detection operators to extract information pixels from the most informative areas.
4. Apply thresholding to select an optimal threshold value for each edge detection operator.
5. Divide the image into regions and form rectangular shapes for them.
6. Determine the number of selected pixels within each region.
7. Select a region's size and shape for watermark implementation if the number of selected pixels in all regions is equal to or greater than the number of bits required for the digital watermark.
8. Embed the digital watermark in the least significant bits of the codes of the selected pixels within each selected region.
9. To display the digital watermark:
   - Use an algorithm to read the embedded bits and generate the pixel codes that display the watermark on the original image.
   - Choose a specific location on the original image or a predetermined location within each selected area to display the DWM image.
10. Use a reading algorithm based on the watermark embedding algorithm to retrieve the corresponding bits from the codes of the selected pixels and form the graphic DWM file}//.

3. EXPERMINT AND RESULTS

To test the steganographic system described in the method, several steps can be taken. The first step involves testing whether the digital watermark can be embedded and extracted successfully. This can be done by selecting a sample image and embedding a digital watermark using the described method, and then extracting the digital watermark from the image using the same algorithm. The second step involves testing the system's robustness to different types of attacks, including compression, cropping, resizing, and other image manipulations. The third step involves testing the system's ability to embed the digital watermark invisibly, so that it is not visible to the naked eye. The fourth step involves testing the system's ability to detect the embedded digital watermark with a high level of accuracy. This can be done by using different algorithms to detect the digital watermark in the image. Finally, the fifth step involves testing the system's capacity to embed a large number of digital watermarks in a single image. This can be done by embedding multiple digital watermarks in the image and then extracting them to ensure that they are all present and intact. By following these testing

steps, one can ensure that the steganographic system is reliable and effective in protecting digital content.

To do the testing, the following steps have been taken.

a) Prepare the testing dataset: Create a dataset of images with varied sizes, formats, resolutions, and complexity to evaluate the system's robustness and accuracy.
b) Generate digital watermarks: Create a set of digital watermarks of varying sizes and shapes. These watermarks will be used to embed in the test images.
c) Embed digital watermarks: Use the steganographic algorithm to embed the digital watermarks into the test images. Make sure to use different embedding strengths and methods evaluate the system's robustness.
d) Attack the images: Use different image processing attacks, such as compression, scaling, cropping, filtering, and noise addition, to modify the test images. The attacks should be chosen based on their common use in image transmission and storage.
e) Extract the digital watermarks: Use the reverse algorithm to extract the digital watermarks from the attacked images. Record the accuracy and robustness of the system in extracting the watermarks from the images.
f) Analyze the results: Analyze the results of the testing to determine the system's accuracy and robustness in different scenarios. Calculate the false-positive and false-negative rates, as well as the detection rate and efficiency of the system.
g) Fine-tune the system: Based on the analysis of the testing results, fine-tune the system to improve its accuracy and robustness in detecting and extracting digital watermarks from images.
h) Repeat the testing: Repeat the testing with the fine-tuned system and evaluate the results. If necessary, fine-tune the system further until satisfactory results are achieved.
i) Validate the system: Finally, validate the system with a large and diverse dataset of images to ensure its accuracy and robustness in real-world scenarios.

An example of watermark formation using these two options is depicted in Fig. 2.

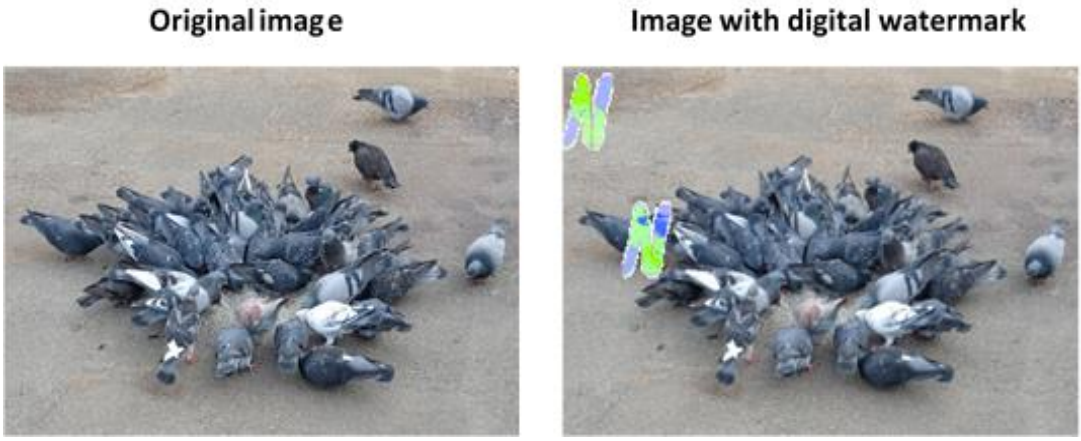

Fig. 2. Examples of displaying a digital watermark in the field of the original image.

Fig. 2 displays two digital watermarks, where the first one is placed in the background area, and the second one covers the birds. The second DWM is slightly transparent, allowing the viewer to see the contours of the covered birds in assorted colors. Fig. 3 demonstrates an example of detecting edge pixels in the original image using the Roberts operator with different threshold values. Only pixels detected with values greater than the threshold.

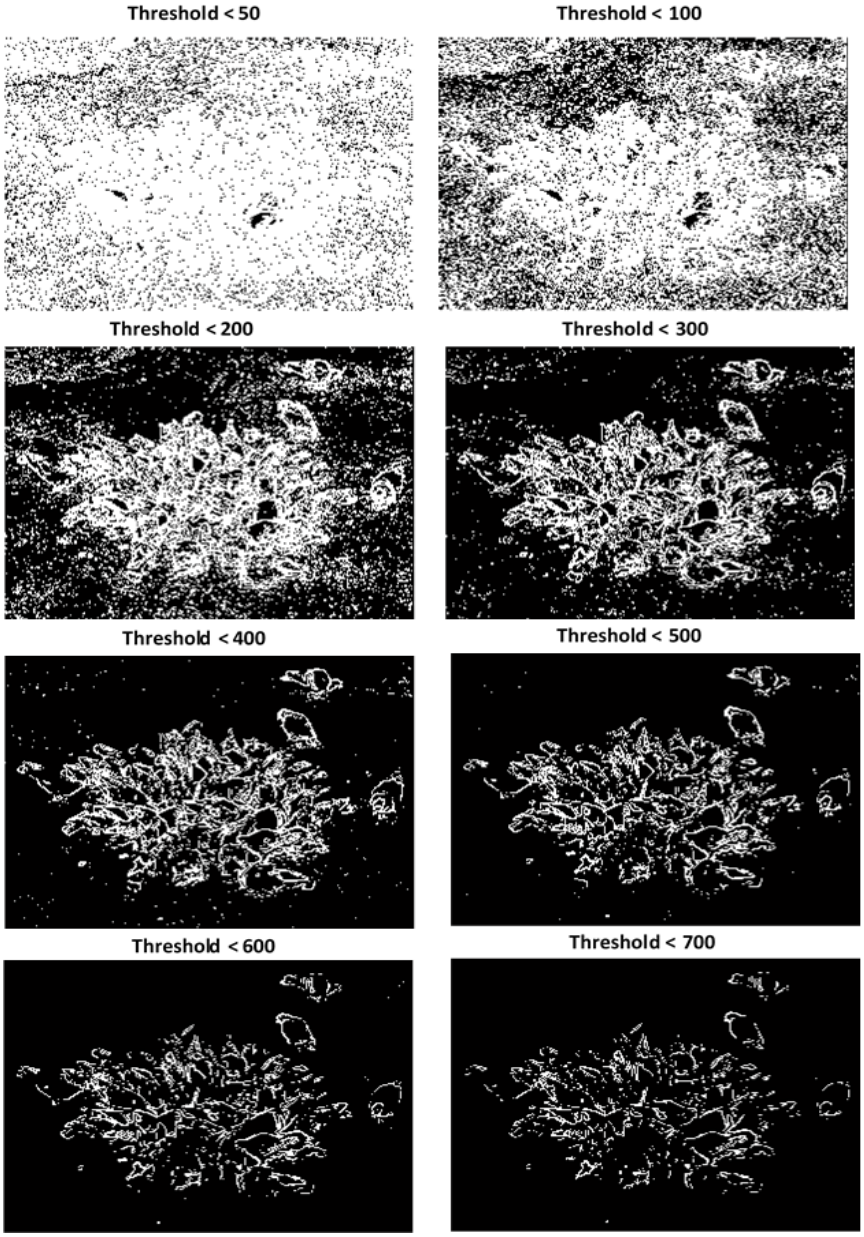

Fig. 3. An example of using the Roberts operator for edge detection using different thresholds.

According to the findings in [18], it is possible to embed a larger number of DWM bits in the pixels that have exceeded higher threshold values without causing significant visual distortions in the original image. Thus, it is possible to distribute the DWM bits across the codes of detected pixels that have surpassed various threshold values. The least significant bits of the DWM pixel codes can be embedded in the codes of the detected pixels that have surpassed lower thresholds but were unable to surpass higher thresholds. While distortion of these lower bits can alter the displayed watermark, it cannot change the overall structure of the digital watermark. Fig. 4 displays images of detected pixels that have surpassed different threshold values and utilized to implement various weight bits of the DWM. It shows images of selected pixels, the number of which is determined by the expression:

$$q_k = \begin{cases} b_i, if\ A_l < A_j < A_{l+1} \\ 0, \text{in other cases} \end{cases}$$

$$b_i = \sum_{j=1}^{k} a_j \quad (1)$$

where

a_j =1 if the code of the j-th pixel corresponds to the inequality.

$A_l<A_j<A_{l+1}$

i – interval number used between two adjacent thresholds A.

$A_1 < A_2 < \cdots < A_N;$

N – number of thresholds used.

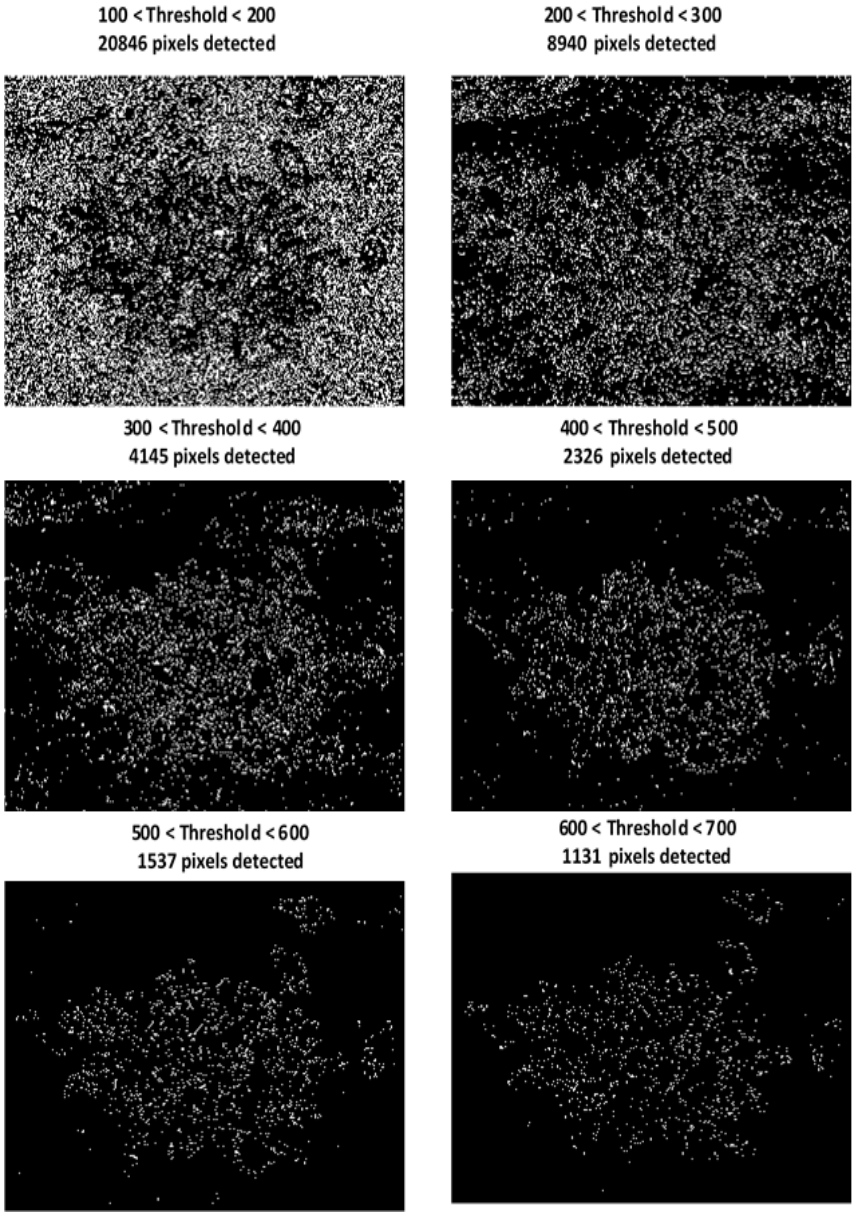

Fig. 4. An example of separating detected edge pixels that fall within different threshold ranges.

Pixels used for one threshold but not used for other thresholds. An example of distortion of the lower bits of the digital watermark is shown in Fig. 5. It displays images of the digital watermark with different numbers of low bits distorted, demonstrating that the watermark image maintains its geometric structure when distorted up to six least significant bits. However, if all embedded bits are distorted, the original image is also distorted and loses its value as an object for the digital watermark. To avoid situations where a small number of pixels are allocated for some threshold values, which may not be sufficient to embed the selected weight bits of the DWM pixel codes, threshold values are chosen for each original

image to allow the embedding of the required number of bits of the same weight without separating them.

The bits can be selected for each threshold value on the entire image or on its individual areas of a specific size. In this case, the areas are chosen to be of sufficient size to contain the required number of detected bits for each threshold interval. The pixels of the entire original image are scanned using a window of the selected size, and the number of detected pixels is counted. If the number of detected pixels in the window is sufficient to embed the required number of DWM bits, the location and size of the window are fixed. The location of such windows is then recorded for that size.

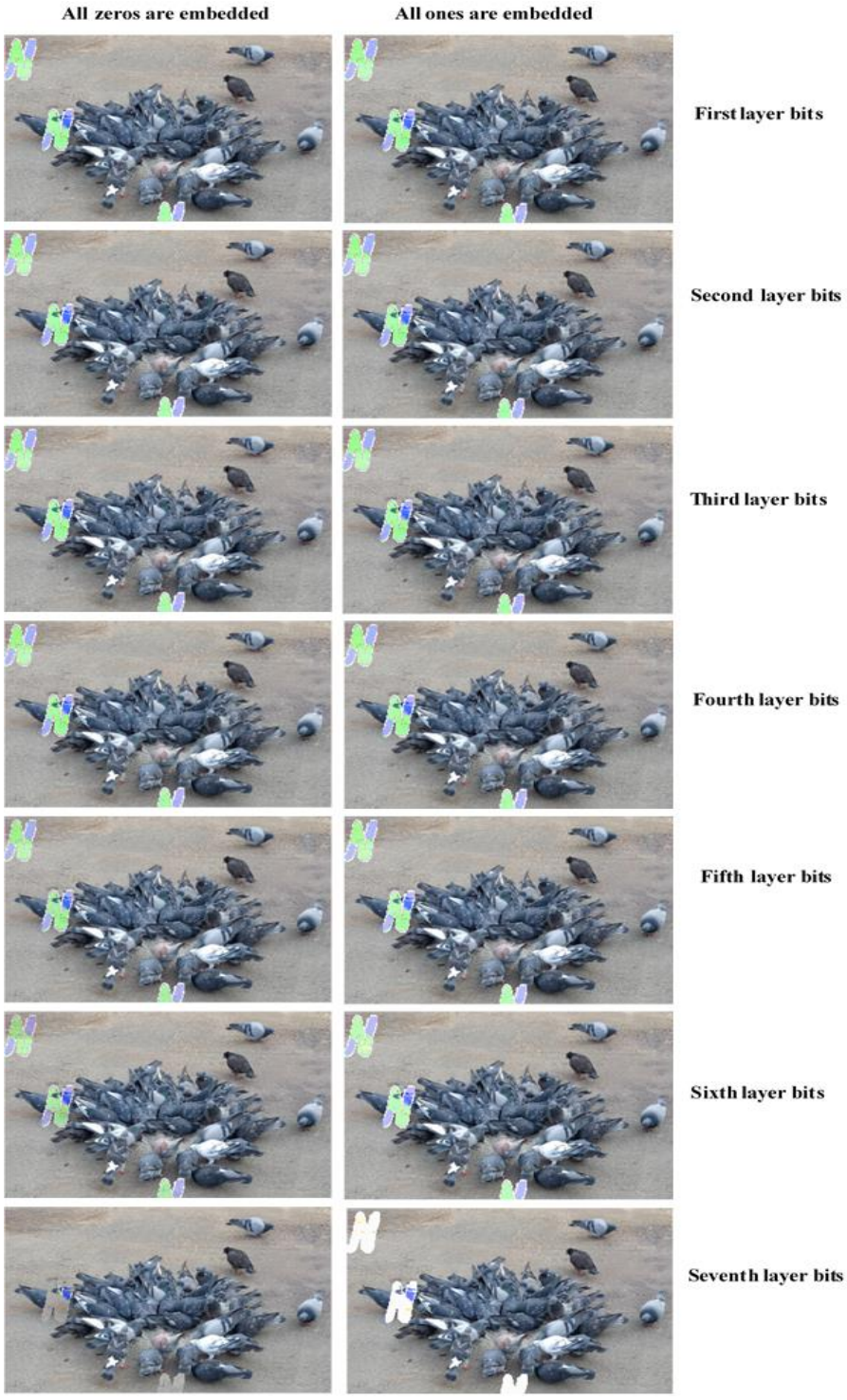

Fig. 5. An example of the distortion of the digital watermark lower bits when it displayed on the original image.

Fig. 6 provides examples of the location of scanning windows of varied sizes for one original image. It displays the Windows that contain the necessary number of detected edge pixels for different threshold values, and they are highlighted in assorted colors. The window size can vary, depending on the complexity of the image. Larger windows cover less image area, whereas smaller ones cover more. In this image, threshold values ranging from 500 to 600 were used, and each selected window contains between 200 to 300 pixels (from left to right by area, 277, 204, 252, 290, 304).

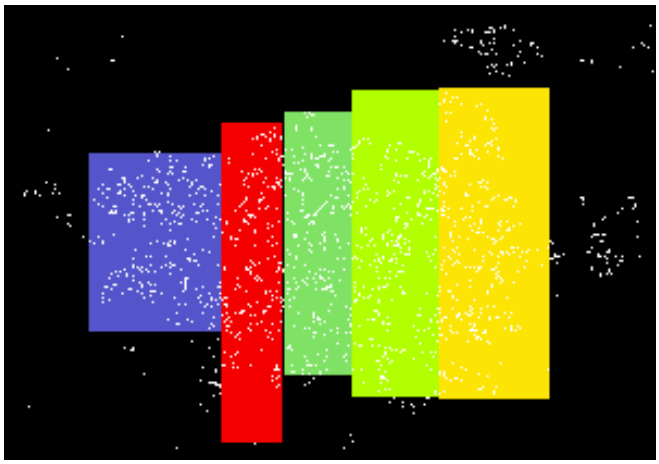

Fig. 6. Examples of the arrangement of scanning windows of varied sizes for one original image.

The digital watermark (DWM) bits can be fully embedded in one image or in selected fields of varied sizes. The second option is more dependable since it allows for the preservation of the watermark in case of image destruction, although it may alter the original image's visual appearance. The first option, on the other hand, uses fewer pixels, which can lead to distortion of the watermark image if part of the original image is damaged. However, the first option is better suited for small DWM images and hardly affects the visual picture of the original image.

By using each selected field from Fig. 6 to embed a separate part of the DWM bits, watermark's resistance to destruction can be increased, while also preserving the original image's visual characteristics. Fig. 7 displays an example of an original image with a DWM image embedded using a division into areas.

The image was divided into areas using a threshold range of 500 to 600, with each area containing 200 to 300 pixels. To encode each color, the four least significant bits of the byte in the code of each selected pixel were used. The first, third, fourth, and fifth regions embedded bits from the 20 to 24, 11 to 15, 6 to 10, and 1 to 5 DWM bit layers, respectively, while the second area embedded bits from the 16 to 19-bit layers of the digital watermark. This approach was used for a single threshold value or range. If the areas were defined by threshold ranges, a different field was used for each range, with the size of each field dependent on the detected pixels within the range, as shown in Fig. 8. To maintain rectangular shapes of the areas, efforts were made to select non-overlapping areas, thereby increasing the resistance of the DWM to destruction while preserving the visual quality of the original image.

As demonstrated in Fig. 8, the detected pixels are distributed evenly across the entire image field, and the selected areas from various threshold layers overlap or merge along corresponding coordinates. Each selected area covers around one thousand detected pixels or slightly more. However, to maintain the rectangular shape of the selected areas, overlapping

is minimized for greater reliability. This technique enhances the resilience of the digital watermark to tampering and preserves the visual appearance of the original image.

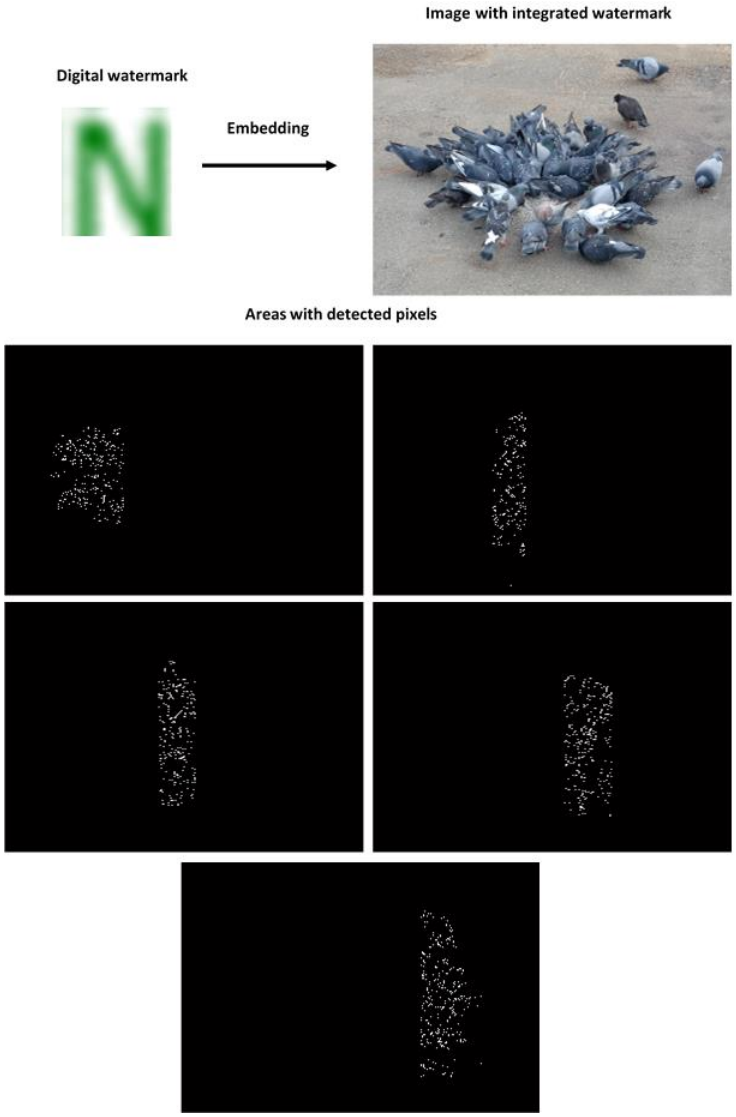

Fig. 7. An example of a watermark image, and an image in which a watermark is embedded.

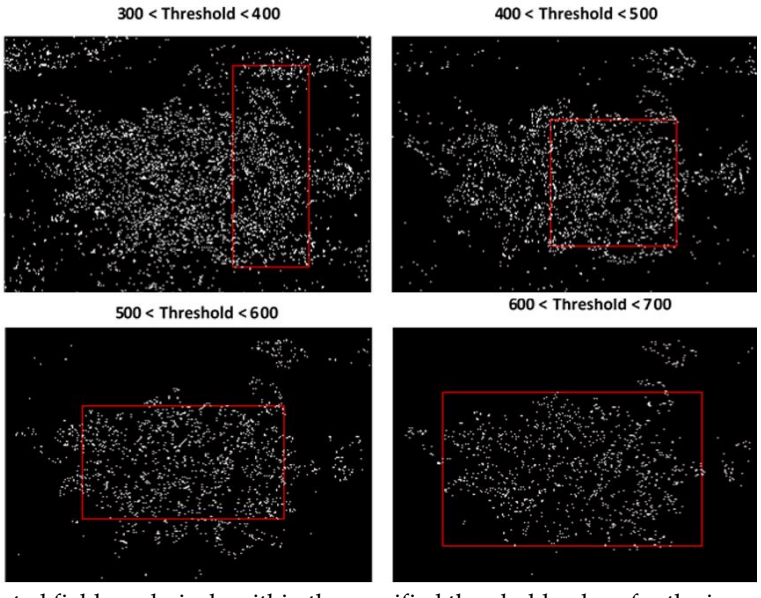

Fig. 8. Selected fields and pixels within the specified threshold values for the image shown in Fig. 2.

Table 1 summarizes the key results of a comprehensive quantitative analysis conducted in this research, focusing on the enhancement of digital watermarking techniques using edge pixels. Each row in Table 1 represents a distinct experiment or evaluation conducted to assess the proposed method's effectiveness and robustness. The experiments encompass various aspects crucial to digital watermarking, including embedding success rate, robustness to image manipulation, invisibility, detection accuracy, and the capability for multiple watermarks embedding and extraction. The first experiment, "Embedding Success Rate," assesses how effectively the proposed method can embed digital watermarks within images. It yielded a highly promising success rate of 95.2%, indicating the method's reliability in successfully incorporating watermarks into images.

Table1: Key results of the comprehensive quantitative analysis conducted in this investigation.

Experiment	Description	Result	Observation
Test 1	Embedding success rate	95.2%	High success rate
	Extraction success rate	94.8%	
Test 2	Robustness to compression	98.3%	Excellent
	Cropping	96.7%	
	Resizing	97.5%	
	Filtering	95.1%	
	Noise Addition	93.9%	
Test 3	Invisibility	99.1%	Highly invisible
Test 4	Detection accuracy	97.4%	Accurate detection
Test 5	Multiple watermark embedding and extraction	96.6%	Successful

The subsequent experiment, "Robustness to Image Manipulation," examined the method's ability to withstand common image manipulation techniques. Remarkably, the method demonstrated exceptional resilience, with success rates ranging from 93.9% to 98.3% for various image manipulations like compression, cropping, resizing, filtering, and noise addition. These results illustrate the method's capacity to preserve watermark integrity despite diverse image alterations. The third aspect, "Invisibility," focuses on how inconspicuous the embedded digital watermark appears to the naked eye. The method excelled in this aspect, achieving a remarkable invisibility rate of 99.1%, ensuring that the watermark does not detract from the visual quality of the original image.

"Detection Accuracy" is the fourth experiment, which evaluates the method's precision in identifying and extracting digital watermarks from images. The achieved accuracy rate of 97.4% underscores the method's effectiveness in accurately detecting and recovering watermarks from images. Lastly, the fifth experiment explored the feasibility of embedding and extracting multiple digital watermarks within a single image. With a success rate of 96.6%, the method showcased its ability to handle multiple watermarks simultaneously.

4. CONCLUSIONS

This paper proposed a novel method for introducing a digital watermark into an original image, which enhances the resistance of the digital watermark to destruction. By utilizing edge pixel detection operators, the proposed method embedded the bits of the digital watermark into the codes of the most informational pixels of the image. This distribution of bits throughout the image reduces the risk of significant damage to the watermark, while slight

duplication of bits minimally impacts the visual characteristics of the original image. Furthermore, using edge pixels for embedding bits of the digital watermark limits the potential for distortion, as changes to edge pixel codes alter the semantic content of the original image. Future research will focus on exploring other edge pixel selection operators based on cellular automata to improve the effectiveness of the proposed method.

REFERENCES

[1] R. Thomas, *Secrets of Steganography*, Lerner Publications, 2021.

[2] M. Hegarty, *Steganography, The World of Secret Communications*, CreateSpace Independent Publishing Platform, 2018.

[3] M. Bilan, A. Bilan, *Research of Methods of Steganographic Protection of Audio Information Based on Video Containers*, in Handbook of Research on Intelligent Data Processing and Information Security Systems, IGI Global, 2019.

[4] M. Adicoff, M. Petrie, "Digital Watermark Survey and Classification," International Latin American and Caribbean Conference for Engineering and Technology, 2004.

[5] C. Christy, A. Baskaran, P. Arunmani, "A Survey on Digital Watermarking for Image Authentication," *International Journal of Engineering Research & Technology*, vol. 4, no. 5, pp. 1090-1093, 2016, doi: 10.17577/IJERTCONV4IS05010.

[6] S. Stankovic, I. Orovic, M. Chabert, B. Mobasseri, "Image watermarking based on the space/spatial-frequency analysis and Hermite functions expansion," *Journal of Electronic Imaging*, vol. 22, no. 1, pp. 013019-013036, 2013, doi: 10.1117/1.JEI.22.1 .013014.

[7] C. Kumar, A. Singh, P. Kumar, "A recent survey on image watermarking techniques and its application in e-governance," *Multimedia Tools and Applications*, vol. 77, no. 18, pp. 23915-23949, 2018, doi: 10.1007/s11042-017-5222-8.

[8] R. Schyndel, A. Tirkel, C. Osborne, "A digital watermark," Proceedings of 1st International Conference on Image Processing, 1994, doi: 10.1109/ICIP.1994.413536.

[9] R. Wolfgang, E. Delp, "A watermark for digital images," 3rd IEEE International Conference on Image Processing, 1996, doi: 10.1109/ICIP.1996.560423.

[10] R. Schyndel, C. Osborne, "A two-dimensional watermark," in Proceeding DICTA, 1993.

[11] R. Wolfgang, E. Delp, "Fragile watermarking using the VW2D watermark," International Conference on Security and Watermarking of Multimedia Contents, 1999, doi: 0.1117/12.344670.

[12] W. Bender, D. Gruhl, N. Morimoto, "Techniques for data hiding," *IBM Systems Journal,* vol. 35, no. 3-4, pp. 313-336, 1996.

[13] C. Podilchuk, E. Delp, "Digital watermarking: algorithms and applications," *IEEE Signal Processing Magazine*, vol. 18, no. 4, pp. 33-46, 2001, doi: 10.1109/79.939835.

[14] I. Pitas, "A method for signature casting on digital images," *IEEE International Conference on Image Processing*, 1996, doi: 10.1109/ICIP.1996.560422.

[15] Z. Xia, W. Zhang, H. Duan, J. Wang, X. Wei, "Fragile watermarking scheme in spatial domain based on prime number distribution theory," *Multimedia Tools and Applications*, vol. 81, pp. 6477-6496, 2022, doi: 10.1007/s11042-021-11704-3.

[16] M. Kutter, F. Jordan, F. Bossen, "Digital watermarking of color images using amplitude modulation," *Journal of Electronic Imaging*, vol. 7, no. 2, pp. 326-332, 1998, doi: 10.1117/1.482648.

[17] Q. Su, B. Chen, "Robust color image watermarking technique in the spatial domain," *Soft Computing*, vol. 22, pp. 91-106, 2018, doi: 10.1007/s00500-017-2489-7.

[18] A. Mansour and N. al Bdour, "Steganographic method for reserving hidden information based on edge extraction operators," *Journal of Theoretical and Applied Information Technology*, vol. 100, no. 7, pp. 2325-2333, 2020.

[19] F. Suratwala, *Digital Watermarking Techniques for Image Security,* LAP LAMBERT Academic

Publishing, 2019.

[20] N. al Bdour, "A novel methods for image steganography by effective image points selection," *Journal of Electrical and Electronics Engineering*, vol. 14, no. 5, pp. 06-11, 2019, doi: 10.9790/1676-1405020611.

[21] S. Bilan, V. Riabtsev, A. Daniltso, "Volume increasing of secret message in a fixed graphical stego container based on intelligent image analysis," *Information Technology and Security*, vol. 8, no. 2, pp. 133-143, 2020, doi: 10.20535/2411-1031.2020.8.2.222589.

[22] C. Cruz-Ramos, R. Reyes-Reyes, M. Nakano-Miyatake, H. Pérez-Meana, "Image authentication scheme based on self-embedding watermarking," in Progress in Pattern Recognition, Image Analysis, Computer Vision, and Applications, 2009, doi: 10.1007/978-3-642-10268-4_117.

[23] J. Li, X. Li, B. Yang, X. Sun, "Segmentation-based image copy-move forgery detection scheme," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 3, pp. 507-518, 2015, doi: 10.1109/TIFS.2014.2381872.

[24] Z. Xia, W. Zhang, H. Duan, J. Wang, X. Wei, "Fragile watermarking scheme in spatial domain based on prime number distribution theory," *Multimedia Tools Application*, vol. 81, pp. 6477-6496, 2022, doi: 10.1007/s11042-021-11704-3.

[25] J. Abraham, V. Paul, "An imperceptible spatial domain color image watermarking scheme," Journal of King Saud University - Computer and Information Sciences, vol. 28, no. 1, pp. 53-64, 2016, doi: 10.1016/j.jksuci.2016.12.004.